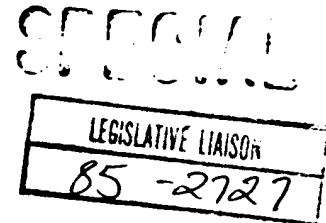




**EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503**

September 17, 1985

LEGISLATIVE REFERRAL MEMORANDUM



TO: Department of Commerce - Mike Levitt (377-3151)
General Services Administration - Ted Ebert (566-1250)
✓ Central Intelligence Agency


SUBJECT: NSA testimony on H.R. 2889, entitled "The Computer Security Research and Training Act of 1985."

The Office of Management and Budget requests the views of your agency on the above subject before advising on its relationship to the program of the President, in accordance with Circular A-19.

Please provide us with your views no later than

2:00 P.M. TODAY, SEPTEMBER 17, 1985.

Direct your questions to Gregory Jones (395-3454), of this office.


for James C. Murr for
Assistant Director for
Legislative Reference

Enclosures

cc: E. Springer
S. Dotson
K. Sheid

Page Denied

Next 8 Page(s) In Document Denied

OLL 85-1999/5
26 July 1985

MEMORANDUM FOR: Director, Office of Security
Chief, Intelligence Law Division, OGC
Chief, Information Handling Committee,
Intelligence Community Staff

STAT

FROM:
Legislation Division
Office of Legislative Liaison

SUBJECT: Computer Security Legislation

REFERENCE: Memo to D/OS and C/ILD from Pearline, dated
16 July, same subject

1. Attached is a proposed response to the request by Congressman Brooks for the Agency's views on H.R. 2889, a bill to establish a computer security research program and to set standards for training personnel in computer security. The proposed response states that while we share the concern of the Congressman over computer security, we cannot endorse the bill because it undercuts an established Administration program to enhance computer security in the federal government. The proposed response also states that the bill should be amended to protect the DCI's authorities if a decision is made to go ahead with the bill despite Administration opposition.

2. I would appreciate receiving your views on this proposed response at the earliest possible time. One area of the proposed response that you should focus on is our general opposition to the bill based on the fact that it overturns NSDD-145 on computer security. Since this NSDD was recently promulgated by the Administration, it is unlikely OMB will approve for transmittal to the Hill a letter that merely excepts the Agency from the scope of the bill, but does not address the fact that the bill totally overturns NSDD-145. For this reason, the attached response addresses both the NSDD and the need to safeguard current DCI authorities in this area.

STAT

Attachment

Page Denied

Next 2 Page(s) In Document Denied

OIT-0584-85

19 JUL 1985

85-1999/2

MEMORANDUM FOR: Director, Office of Legislative Liaison

FROM:

[Redacted]

Deputy Director for Management, OIT

SUBJECT: Response to Congressional Bill HR 2889

25X1

The Office of Information Technology believes language should be added to HR 2889 to protect DCI authorities, to wit: "Nothing in this Bill should be construed as altering the existing authorities of the Director of Central Intelligence, including his responsibilities for the protection of intelligence sources and methods."

[Redacted]

SECRET

July 19, 1985

25X1 NOTE FOR: [REDACTED] 25X1
CIA/OLL, Rm. 7B14, HQ.
25X1 FROM: [REDACTED] 25X1
IC Staff/Information Handling Committee
SUBJECT: Attached H.R. 2889/NSDD 145 Package

25X1 1. [REDACTED] Chairman of the Information Handling Committee, asked 25X1
me to send you a copy of the package that we sent up to the Director and
Deputy Director/ICS a few days ago. I have also included a copy of NSDD 145
and the hearings on computer security policies for your background information
in this area.

25X1 2. If you have any questions, please call me on [REDACTED] 25X1

25X1 [REDACTED] 25X1
[REDACTED]

Attachments

Downgrade to UNCLASSIFIED upon
removal of attachments.

SECRET

NSDD 145

SECRET

9216/1-84

ER ~~SECRET~~

No. NSDD 145

COPY 3 LC Ser B

NATIONAL SECURITY COUNCIL INFORMATION

REPRODUCE ONLY
With Permission
of EO/ICS

25X1

25X1
ILLEGIB

Notice

The attached document contains classified National Security Council Information. It is to be read and discussed only by persons authorized by law.

Your signature acknowledges you are such a person and you promise you will show or discuss information contained in the document only with persons who are authorized by law to have access to this document.

Persons handling this document acknowledge he or she knows and understands the security law relating thereto and will cooperate fully with any lawful investigation by the United States Government into any unauthorized disclosure of classified information contained herein.

ILLEGIB

Access List

DATE

NAME

DATE

NAME

ILLEGIB

25X1

SECRET

SECRET

90078

THE WHITE HOUSE

WASHINGTON

SECRET/WITH CONFIDENTIAL ATTACHMENT

Executive Registry

84- 9216/1

September 17, 1984

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF TRANSPORTATION
THE SECRETARY OF ENERGY
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
THE DIRECTOR OF CENTRAL INTELLIGENCE
CHAIRMAN, JOINT CHIEFS OF STAFF
ADMINISTRATOR, GENERAL SERVICES ADMINISTRATION
DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
DIRECTOR, FEDERAL EMERGENCY MANAGEMENT AGENCY
THE CHIEF OF STAFF, UNITED STATES ARMY
THE CHIEF OF NAVAL OPERATIONS
THE CHIEF OF STAFF, UNITED STATES AIR FORCE
COMMANDANT, UNITED STATES MARINE CORPS
DIRECTOR, DEFENSE INTELLIGENCE AGENCY
DIRECTOR, NATIONAL SECURITY AGENCY
MANAGER, NATIONAL COMMUNICATIONS SYSTEM

SUBJECT: National Policy on Telecommunications and
Automated Information Systems Security (U)

The President has approved and signed the attached National Security Decision Directive which establishes initial national objectives, policies and an improved organizational structure for protecting US telecommunications and automated information systems from exploitation by hostile intelligence activities.
(U)

The Secretary of Defense's recent biennial report to the President on the security of US Government communications concludes that when viewed from a national perspective, the security of our communications is perilous and that intelligence available to hostile intelligence services through unprotected or inadequately protected US communications is unsurpassed for its timeliness, accuracy, completeness and affects every aspect of our national security. This NSDD establishes a means by which the government can develop measures to adequately secure our communications. (S)

SECRET/WITH CONFIDENTIAL ATTACHMENT

COPY 11 OF 22 COPIES

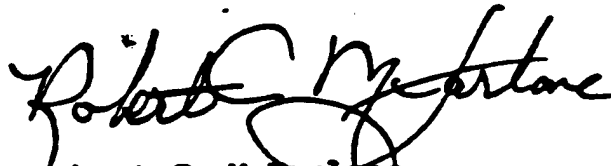
2

SECRET/WITH CONFIDENTIAL ATTACHMENT

In order to begin this vital task, the Chairman of the National Communications Security Committee (NCSC) is requested to immediately expand the NCSC into the new National Telecommunications and Information Systems Security Committee (NTISSC) and prepare an initial plan for implementation of the NSDD for submission to the steering group by October 1, 1984. (U)

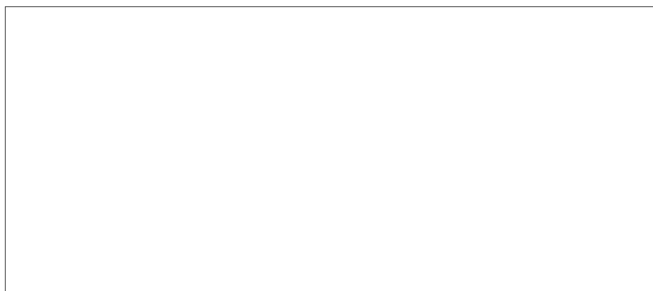
Authority for distributing additional copies of the NSDD to appropriate agencies throughout the government will be provided to the Chairman of the NTISSC and the Manager, National Communications Systems, in the near future. (U)

FOR THE PRESIDENT:


Robert C. McFarlane

Attachment
National Security
Decision Directive 145

25X1



SECRET/WITH CONFIDENTIAL ATTACHMENT

PAGE // OF 22 PAGES

CONFIDENTIAL

90078

THE WHITE HOUSE**WASHINGTON****CONFIDENTIAL****September 17, 1984****Executive Registry****84- 9216****National Security Decision
Directive Number 145****NATIONAL POLICY ON TELECOMMUNICATIONS
AND AUTOMATED INFORMATION SYSTEMS SECURITY (U)**

Recent advances in microelectronics technology have stimulated an unprecedented growth in the supply of telecommunications and information processing services within the government and throughout the private sector. As new technologies have been applied, traditional distinctions between telecommunications and automated information systems have begun to disappear. Although this trend promises greatly improved efficiency and effectiveness, it also poses significant security challenges. Telecommunications and automated information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation, as well as other dimensions of the hostile intelligence threat. The technology to exploit these electronic systems is widespread and is used extensively by foreign nations and can be employed, as well, by terrorist groups and criminal elements. Government systems as well as those which process the private or proprietary information of US persons and businesses can become targets for foreign exploitation. (U)

Within the government these systems process and communicate classified national security information and other sensitive information concerning the vital interests of the United States. Such information, even if unclassified in isolation, often can reveal highly classified and other sensitive information when taken in aggregate. The compromise of this information, especially to hostile intelligence services, does serious damage to the United States and its national security interests. A comprehensive and coordinated approach must be taken to protect the government's telecommunications and automated information systems against current and projected threats. This approach must include mechanisms for formulating policy, for overseeing systems security resources programs, and for coordinating and executing technical activities. (U)

This Directive: Provides initial objectives, policies, and an organizational structure to guide the conduct of national activities directed toward safeguarding systems which process or communicate sensitive information from hostile exploitation; establishes a mechanism for policy development; and assigns

CONFIDENTIAL**CONFIDENTIAL****COPY 11 DE 22 COPIES**

CONFIDENTIAL

responsibilities for implementation. It is intended to assure full participation and cooperation among the various existing centers of technical expertise throughout the Executive Branch, to promote a coherent and coordinated defense against the hostile intelligence threat to these systems, and to foster an appropriate partnership between government and the private sector in attaining these goals. This Directive specifically recognizes the special requirements for protection of intelligence sources and methods. It is intended that the mechanisms established by this Directive will initially focus on those automated information systems which are connected to telecommunications transmission systems. (U)

1. Objectives. Security is a vital element of the operational effectiveness of the national security activities of the government and of military combat readiness. Assuring the security of telecommunications and automated information systems which process and communicate classified national security information, and other sensitive government national security information, and offering assistance in the protection of certain private sector information are key national responsibilities. I, therefore, direct that the government's capabilities for securing telecommunications and automated information systems against technical exploitation threats be maintained or improved to provide for:

a. A reliable and continuing capability to assess threats and vulnerabilities, and to implement appropriate, effective countermeasures.

b. A superior technical base within the government to achieve this security, and support for a superior technical base within the private sector in areas which complement and enhance government capabilities.

c. A more effective application of government resources and encouragement of private sector security initiatives.

d. Support and enhancement of other policy objectives for national telecommunications and automated information systems., (U)

2. Policies. In support of these objectives, the following policies are established:

a. Systems which generate, store, process, transfer or communicate classified information in electrical form shall be secured by such means as are necessary to prevent compromise or exploitation.

b. Systems handling other sensitive, but unclassified, government or government-derived information, the loss of which could adversely affect the national security interest,

CONFIDENTIAL**CONFIDENTIAL**

COPY # DE 22 COPIES

CONFIDENTIAL**CONFIDENTIAL**

shall be protected in proportion to the threat of exploitation and the associated potential damage to the national security.

c. The government shall encourage, advise, and, where appropriate, assist the private sector to: identify systems which handle sensitive non-government information, the loss of which could adversely affect the national security; determine the threat to, and vulnerability of, these systems; and formulate strategies and measures for providing protection in proportion to the threat of exploitation and the associated potential damage. Information and advice from the perspective of the private sector will be sought with respect to implementation of this policy. In cases where implementation of security measures to non-governmental systems would be in the national security interest, the private sector shall be encouraged, advised, and, where appropriate, assisted in undertaking the application of such measures.

d. Efforts and programs begun under PD-24 which support these policies shall be continued. (U)

3. Implementation. This Directive establishes a senior level steering group; an interagency group at the operating level; an executive agent and a national manager to implement these objectives and policies. (U)

4. Systems Security Steering Group.

a. A Systems Security Steering Group consisting of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Director of the Office of Management and Budget, the Director of Central Intelligence, and chaired by the Assistant to the President for National Security Affairs is established. The Steering Group shall:

(1) Oversee this Directive and ensure its implementation. It shall provide guidance to the Executive Agent and through him to the National Manager with respect to the activities undertaken to implement this Directive.

(2) Monitor the activities of the operating level National Telecommunications and Information Systems Security Committee and provide guidance for its activities in accordance with the objectives and policies contained in this Directive.

(3) Review and evaluate the security status of those telecommunications and automated information systems that handle classified or sensitive government or government-derived information with respect to established objectives and priorities, and report findings and recommendations through the National Security Council to the President.

CONFIDENTIAL

COPY 11 DE 22 COPIES

~~CONFIDENTIAL~~CONFIDENTIAL

(4) Review consolidated resources program and budget proposals for telecommunications systems security, including the COMSEC Resources Program, for the US Government and provide recommendations to OMB for the normal budget review process.

(5) Review in aggregate the program and budget proposals for the security of automated information systems of the departments and agencies of the government.

(6) Review and approve matters referred to it by the Executive Agent in fulfilling the responsibilities outlined in paragraph 6. below.

(7) On matters pertaining to the protection of intelligence sources and methods be guided by the policies of the Director of Central Intelligence.

(8) Interact with the Steering Group on National Security Telecommunications to ensure that the objectives and policies of this Directive and NSDD-97, National Security Telecommunications Policy, are addressed in a coordinated manner.

(9) Recommend for Presidential approval additions or revisions to this Directive as national interests may require.

(10) Identify categories of sensitive non-government information, the loss of which could adversely affect the national security interest, and recommend steps to protect such information. (U)

b. The National Manager for Telecommunications and Information Systems Security shall function as executive secretary to the Steering Group. (U)

5. The National Telecommunications and Information Systems Security Committee.

a. The National Telecommunications and Information Systems Security Committee (NTISSC) is established to operate under the direction of the Steering Group to consider technical matters and develop operating policies as necessary to implement the provisions of this Directive. The Committee shall be chaired by the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) and shall be composed of a voting representative of each member of the Steering Group and of each of the following:

→ The Secretary of Commerce
The Secretary of Transportation
The Secretary of Energy

COPY 11 OF 22 COPIES

~~CONFIDENTIAL~~~~CONFIDENTIAL~~

CONFIDENTIAL**CONFIDENTIAL**

Chairman, Joint Chiefs of Staff
 Administrator, General Services Administration
 Director, Federal Bureau of Investigation
 Director, Federal Emergency Management Agency
 The Chief of Staff, United States Army
 The Chief of Naval Operations
 The Chief of Staff, United States Air Force
 Commandant, United States Marine Corps
 Director, Defense Intelligence Agency
 Director, National Security Agency
 Manager, National Communications System (U)

b. The Committee shall:

(1) Develop such specific operating policies, objectives, and priorities as may be required to implement this Directive.

(2) Provide telecommunication and automated information systems security guidance to the departments and agencies of the government.

(3) Submit annually to the Steering Group an evaluation of the status of national telecommunications and automated information systems security with respect to established objectives and priorities.

(4) Identify systems which handle sensitive, non-government information, the loss and exploitation of which could adversely affect the national security interest, for the purpose of encouraging, advising and, where appropriate, assisting the private sector in applying security measures.

(5) Approve the release of sensitive systems technical security material, information, and techniques to foreign governments or international organizations with the concurrence of the Director of Central Intelligence for those activities which he manages.

(6) Establish and maintain a national system for promulgating the operating policies, directives, and guidance which may be issued pursuant to this Directive.

(7) Establish permanent and temporary subcommittees as necessary to discharge its responsibilities.

(8) Make recommendations to the Steering Group on Committee membership and establish criteria and procedures for permanent observers from other departments or agencies affected by specific matters under deliberation, who may attend meetings upon invitation of the Chairman.

(9) Interact with the National Communications System Committee of Principals established by Executive Order

CONFIDENTIAL

CONFIDENTIAL

12472 to ensure the coordinated execution of assigned responsibilities. (U)

c. The Committee shall have two subcommittees, one focusing on telecommunications security and one focusing on automated information systems security. The two subcommittees shall interact closely and any recommendations concerning implementation of protective measures shall combine and coordinate both areas where appropriate, while considering any differences in the level of maturity of the technologies to support such implementation. However, the level of maturity of one technology shall not impede implementation in other areas which are deemed feasible and important. (U)

d. The Committee shall have a permanent secretariat composed of personnel of the National Security Agency and such other personnel from departments and agencies represented on the Committee as are requested by the Chairman. The National Security Agency shall provide facilities and support as required. Other departments and agencies shall provide facilities and support as requested by the Chairman. (U)

6. The Executive Agent of the Government for Telecommunications and Information Systems Security. The Secretary of Defense is the Executive Agent of the Government for Communications Security under authority of Executive Order 12333. By authority of this Directive he shall serve an expanded role as Executive Agent of the Government for Telecommunications and Automated Information Systems Security and shall be responsible for implementing, under his signature, the policies developed by the NTISSC. In this capacity he shall act in accordance with policies and procedures established by the Steering Group and the NTISSC to:

a. Ensure the development, in conjunction with NTISSC member departments and agencies, of plans and programs to fulfill the objectives of this Directive, including the development of necessary security architectures.

b. Procure for and provide to departments and agencies of the government and, where appropriate, to private institutions (including government contractors) and foreign governments, technical security material, other technical assistance, and other related services of common concern, as required to accomplish the objectives of this Directive.

c. Approve and provide minimum security standards and doctrine, consistent with provisions of the Directive.

d. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

CONFIDENTIAL**CONFIDENTIAL**COPY 11 OF 22 COPIES

CONFIDENTIAL

7

e. Operate, or coordinate the efforts of, government technical centers related to telecommunications and automated information systems security.

f. Review and assess for the Steering Group the proposed telecommunications systems security programs and budgets for the departments and agencies of the government for each fiscal year and recommend alternatives, where appropriate. The views of all affected departments and agencies shall be fully expressed to the Steering Group.

g. Review for the Steering Group the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for each fiscal year. (U)

7. The National Manager for Telecommunications Security and Automated Information Systems Security. The Director, National Security Agency is designated the National Manager for Telecommunications and Automated Information Systems Security and is responsible to the Secretary of Defense as Executive Agent for carrying out the foregoing responsibilities. In fulfilling these responsibilities the National Manager shall have authority in the name of the Executive Agent to:

a. Examine government telecommunications systems and automated information systems and evaluate their vulnerability to hostile interception and exploitation. Any such activities, including those involving monitoring of official telecommunications, shall be conducted in strict compliance with law, Executive Orders and applicable Presidential Directives. No monitoring shall be performed without advising the heads of the agencies, departments, or services concerned.

b. Act as the government focal point for cryptography, telecommunications systems security, and automated information systems security.

c. Conduct, approve, or endorse research and development of techniques and equipment for telecommunications and automated information systems security for national security information.

d. Review and approve all standards, techniques, systems and equipments for telecommunications and automated information systems security.

e. Conduct foreign communications security liaison, including agreements with foreign governments and with international and private organizations for telecommunications and automated information systems security, except for those foreign intelligence relationships conducted for intelligence purposes by the Director of Central Intelligence. Agreements shall be coordinated with affected departments and agencies.

CONFIDENTIAL**CONFIDENTIAL**

COPY 11 DE 22 COPIES

CONFIDENTIAL

8

f. Operate such printing and fabrication facilities as may be required to perform critical functions related to the provision of cryptographic and other technical security material or services.

g. Assess the overall security posture and disseminate information on hostile threats to telecommunications and automated information systems security.

h. Operate a central technical center to evaluate and certify the security of telecommunications systems and automated information systems.

i. Prescribe the minimum standards, methods and procedures for protecting cryptographic and other sensitive technical security material, techniques, and information.

j. Review and assess annually the telecommunications systems security programs and budgets of the departments and agencies of the government, and recommend alternatives, where appropriate, for the Executive Agent and the Steering Group.

k. Review annually the aggregated automated information systems security program and budget recommendations of the departments and agencies of the US Government for the Executive Agent and the Steering Group.

l. Request from the heads of departments and agencies such information and technical support as may be needed to discharge the responsibilities assigned herein.

m. Enter into agreements for the procurement of technical security material and other equipment, and their provision to government agencies and, where appropriate, to private organizations, including government contractors, and foreign governments. (U)

8. The Heads of Federal Departments and Agencies shall:

a. Be responsible for achieving and maintaining a secure posture for telecommunications and automated information systems within their departments or agencies.

b. Ensure that the policies, standards and doctrines issued pursuant to this Directive are implemented within their departments or agencies.

c. Provide to the Systems Security Steering Group, the NTISSC, Executive Agent, and the National Manager, as appropriate, such information as may be required to discharge responsibilities assigned herein, consistent with relevant law, Executive Order, and Presidential Directives. (U)

CONFIDENTIAL**CONFIDENTIAL**

MDX // 22

CONFIDENTIAL

9

9. Additional Responsibilities.

a. The Secretary of Commerce, through the Director, National Bureau of Standards, shall issue for public use such Federal Information Processing Standards for the security of information in automated information systems as the Steering Group may approve. The Manager, National Communications System, through the Administrator, General Services Administration, shall develop and issue for public use such Federal Telecommunications Standards for the security of information in telecommunications systems as the National Manager may approve. Such standards, while legally applicable only to Federal Departments and Agencies, shall be structured to facilitate their adoption as voluntary American National Standards as a means of encouraging their use by the private sector.

b. The Director, Office of Management and Budget, shall:

(1) Specify data to be provided during the annual budget review by the departments and agencies on programs and budgets relating to telecommunications systems security and automated information systems security of the departments and agencies of the government.

(2) Consolidate and provide such data to the National Manager via the Executive Agent.

(3) Review for consistency with this Directive, and amend as appropriate, OMB Circular A-71 (Transmittal Memorandum No. 1), OMB Circular A-76, as amended, and other OMB policies and regulations which may pertain to the subject matter herein. (U)

10. Nothing in this Directive:

a. Alters the existing authorities of the Director of Central Intelligence, including his responsibility to act as Executive Agent of the Government for technical security countermeasures (TSCM).

b. Provides the NTISSC, the Executive Agent, or the National Manager authority to examine the facilities of other departments and agencies without approval of the head of such department or agency, nor to request or collect information concerning their operation for any purpose not provided for herein.

c. Amends or contravenes the provisions of existing law, Executive Orders, or Presidential Directives which pertain to the privacy aspects or financial management of automated information systems or to the administrative requirements for safeguarding such resources against fraud, abuse, and waste.

CONFIDENTIAL**CONFIDENTIAL**COPY 11 OF 22 COPIES

d. Is intended to establish additional review processes for the procurement of automated information processing systems. (U)

11. For the purposes of this Directive, the following terms shall have the meanings indicated:

a. Telecommunications means the preparation, transmission, communication or related processing of information by electrical, electromagnetic, electromechanical, or electro-optical means.

b. Automated Information Systems means systems which create, prepare, or manipulate information in electronic form for purposes other than telecommunication, and includes computers, word processing systems, other electronic information handling systems, and associated equipment.

c. Telecommunications and Automated Information Systems Security means protection afforded to telecommunications and automated information systems, in order to prevent exploitation through interception, unauthorized electronic access, or related technical intelligence threats, and to ensure authenticity. Such protection results from the application of security measures (including cryptosecurity, transmission security, emission security, and computer security) to systems which generate, store, process, transfer, or communicate information of use to an adversary, and also includes the physical protection of sensitive technical security material and sensitive technical security information.

d. Technical security material means equipment, components, devices, and associated documentation or other media which pertain to cryptography, or to the securing of telecommunications and automated information systems. (U)

12. The Interagency Committee on Real Estate Acquisitions (ICREA) in the United States established under PD-24 shall be reconstituted under the chairmanship of the Director, Office of Foreign Missions, Department of State, with representation from the Department of Defense, the Department of Justice/Federal Bureau of Investigation, the Director of Central Intelligence, the National Security Agency, and the Assistant to the President for National Security Affairs. The Committee, with advice from the Reciprocity Policy Committee of the Department of State, shall provide policy guidance for implementation by the Office of Foreign Missions or other appropriate organizations, on proposals for foreign real estate acquisitions by lease or purchase, that present a threat to US [redacted] systems security [redacted] (C)

13. The functions of the Interagency Group for Telecommunications Protection and the National Communications

CONFIDENTIAL

CONFIDENTIAL

COPY 11 OF 22 COPIES

25X1
25X1

CONFIDENTIAL**11**

Security Committee (NSC) as established under PD-24 are subsumed by the Systems Security Steering Group and the NTISSC, respectively. The policies established under the authority of the Interagency Group or the NSC; which have not been superseded by this Directive, shall remain in effect until modified or rescinded by the Steering Group or the NTISSC, respectively. (U)

14. Except for ongoing telecommunications protection activities mandated by and pursuant to PD/NSC-24, that Directive is hereby superseded and cancelled. (U)

Ronald Reagan

ILLEGIB

CONFIDENTIAL**CONFIDENTIAL**COPY 11 OF 22 COPIES

ADMINISTRATIVE - INTERNAL USE ONLY

17 JUL 1985

MEMORANDUM FOR: Legislative Division, OLL

ATTN:

FROM:

Director of Security

SUBJECT: H.R. 2889 - Computer Security Legislation

REFERENCE: OLL Memo OLL85-1999/1, dtd 16 July 1985,
Same Subject

1. It is recommended that the following clause be proposed for inclusion in H.R. 2889:

"Nothing in this bill alters the existing authorities of the Director of Central Intelligence, including his responsibilities for the protection of intelligence sources and methods."

2. The Office of Security has no objection to the stated intent of the bill, since there is unquestionably a need for greater emphasis on computer security throughout the government. The bill does not appear to represent a potential for negative effects on the Agency's computer security program.

3. Interaction between the Office of Security and the Office of Personnel Management (OPM) has been generally favorable. Most computer security officers attend OPM computer security training courses. It is not believed that OPM government-wide standards would present any particular problems for the Agency.

4. The Office of Security is in agreement with the tone of the response proposed in paragraph two of your memorandum.

OS 5 2164

ADMINISTRATIVE - INTERNAL USE ONLY

OLL85-1999/1
16 July 1985

MEMORANDUM FOR: Director, Office of Security
Chief, Intelligence Law Division, CGC

FROM:

Legislation Division/CLL

SUBJECT: Computer Security Legislation

1. Congressman Jack Brooks, Chairman, House Government Operations Committee, has requested the Agency to provide its views on H.R. 2889, a bill to establish a computer security training program. The purpose of the bill is to enhance computer security in the federal government. The bill provides for the National Bureau of Standards to establish a computer security research program to address the problems of computer security in the federal government. The bill also provides that each federal agency furnish mandatory periodic training in computer security for all employees who are involved with the management, use or operation of computers or other automated information systems. The details and scope of the training would be prescribed by OPM. Attached is a copy of the bill.

2. I propose responding to Congressman Brooks by applauding his effort to increase computer security in government. The Agency should point out that it has underway a vigorous program to educate its employees on computer security and to provide hardware and software to prevent the unauthorized accessing of Agency computers. One issue that we need to address is whether to concur in the provision of the bill permitting OPM to dictate the scope and manner of the Agency's training of personnel in computer security.

3. I would appreciate having your views on this bill no later than 18 July. I will incorporate your comments into the Agency letter back to the Congressman and circulate that letter to you before final transmittal to the Congressman.

Attachment as stated

25X1

25X1

Distribution:

Original - Addressee(s)

1 - D/OLL

1 - DD/OLL

1 - OLL Chrono

1 - OLL Leg/Subject:

1 - DMP/Signer

STAT

OLL/LEG



ap (16 July 1985)

25X1

99TH CONGRESS
1ST SESSION

H. R. 2889

To amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems.

IN THE HOUSE OF REPRESENTATIVES

JUNE 27, 1985

Mr. GLICKMAN (for himself, Mr. FUQUA, Mr. BROOKS, Mr. BROWN of California, Mr. WIRTH, Mr. WALGREEN, Mr. NELSON of Florida, Mr. WYDEN, Mr. HUGHES, Mr. LEWIS of Florida, and Mr. HORTON) introduced the following bill; which was referred jointly to the Committees on Science and Technology and Government Operations

A BILL

To amend the Act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the "Computer S-

5 Research and Training Act of 1985."

1 SECTION 2 FINDINGS.

2 The Congress finds that—

3 (1) in recent years the Federal Government has
4 become highly dependent on automated information
5 processing systems for carrying out many of its
6 missions.

7 (2) the Government operates about 20,000
8 medium- and large-scale mainframe computers, and by
9 the end of this decade it will also have approximately
10 half a million micro- and mini-computers;

11 (3) the information stored in Government comput-
12 ers and transmitted over the various communications
13 networks that connect them represent valued property
14 that is vulnerable to unauthorized access and disclo-
15 sure, fraudulent manipulation, and disruption;

16 (4) studies of computer-related fraud and abuse in
17 Government agencies indicate a costly and widespread
18 problem of significant proportions;

19 (5) Government efforts to address the problems of
20 computer security have focused on developing hard-
21 ware and software systems to protect sensitive infor-
22 mation, ensuring that new computer systems are de-
23 signed to include security provisions, and requiring
24 agencies to implement security procedures and

(6) these efforts are

1 the information stored, processed, and transmitted by
2 Government computers remains the property of the Government
3 and shall be managed, used, and operated by the Government.

4 **SEC. 3. ESTABLISHMENT OF COMPUTER SECURITY RESEARCH**
5 **PROGRAM.**

6 The Act of March 3, 1959 (41 U.S.C. 171-177), as amended
7 by redesignating section 18 as section 19, and by
8 inserting after section 17 the following new section:

9 "SEC. 18. (a) The National Bureau of Standards shall
10 establish and conduct a computer security research program
11 to address the problems of computer security in the Federal
12 Government, with primary emphasis upon the prevention of
13 computer-related fraud and abuse through the training of em-
14 ployees in computer security awareness and good security
15 practice.

16 "(b) The program shall—

17 "(1) perform research and conduct studies to de-
18 termine the nature and extent of computer security
19 vulnerability in Federal agencies and their contractors;

20 "(2) devise administrative, management, and tech-
21 nical procedures and practices designed to protect the
22 information stored, processed, and transmitted by
23 Government computers; and

24 "(3) develop guidelines for use by Federal agen-
25 cies in training their employees, and the employees of

1 their contractors and of other organizations whose
2 computers interface with Government computers, in
3 computer security awareness and good security
4 practice."

5 SEC. 4. TRAINING BY FEDERAL AGENCIES IN COMPUTER
6 SECURITY.

7 (a) IN GENERAL.—Each Federal agency shall provide
8 mandatory periodic training in computer security, under the
9 guidelines developed pursuant to section 184083 of the Act
10 of March 3, 1901 (as added by section 3 of this Act), and in
11 accordance with the regulations issued under subsection (c) of
12 this section, for all of its employees who are involved with
13 the management, use, or operation of computers or other
14 automated information systems and for all of the employees
15 and other personnel of its contractors who are involved with
16 the management, use, or operation of computers which inter-
17 face with Government computers.

18 (b) **TRAINING OBJECTIVES.**—Training under this sec-
19 tion shall begin within 60 days after the issuance of the regu-
20 lations described in subsection (c), and shall be designed—

21 (1) to enhance employees' awareness of the
22 threats to and vulnerability of computer and communi-
23 cations systems; and

24 (2) to encourage the use of improved computer-
25 security practices at Government facilities.

1 (c) REGULATIONS.—Within six months after the date of
2 the enactment of this Act, the Director of the Office of Per-
3 sonnel Management shall issue regulations prescribing in
4 detail the procedures and scope of the training to be provided
5 by Federal agencies under subsection (a) and the manner in
6 which such training is to be carried out.

7 SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

8 There are hereby authorized to be appropriated to the
9 National Bureau of Standards for the fiscal year 1987, to
10 carry out the computer security research program under sec-
11 tion 18 of the Act of March 3, 1901 (as added by section 3 of
12 this Act), such sums as may be necessary.

○